HSR London International Conference on Multidisciplinary Academic Research
(HSR-ICMAR) 2026
https://houghtonstreetreview.com/index.php/conference

DIGITAL SELF-DETERMINATION AS A FUNDAMENTAL CONSTITUTIONAL PRINCIPLE FOR DATA RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE

Abhijith A.S
National Forensic Sciences University, India
Tashkent State University of Law, Uzbekistan

Islombek Abdikhakimov
Under the Supervision of Dr.

Abstract

The rapid evolution of Artificial Intelligence (AI) has radically altered the relationship between human beings and personal data. Rather than merely storing or retrieving historical records, modern machine learning systems actively infer, predict, classify and evaluate human behaviour, transforming passive datasets into instruments of structural governance. This study evaluates the concept of digital self-determination as a fundamental constitutional principle necessary to preserve human agency, dignity and autonomy against expanding algorithmic power. Through a comparative analysis of three distinct legal landscapes which includes Germany's mature constitutional doctrine of informational self-determination, India's evolving data privacy framework following the landmark Puttaswamy judgment and the Digital Personal Data Protection (DPDP) Act of 2023 and Uzbekistan's emerging statutory and ethical AI governance regimes highlights critical gaps between constitutional aspirations and legislative realities. It argues that traditional notice and consent mechanisms are structurally inadequate in complex algorithmic environments. Instead, a higher order constitutional principle of digital self-determination must be institutionalized globally to address both individual and collective algorithmic harms, ensuring that the human person remains the normative centre of digital governance.

Keywords: Digital Self-Determination, Artificial Intelligence Governance, Informational Privacy, Data Protection, Digital Personal Data Protection Act (DPDP)

Introduction

The contemporary relationship between human beings and digital information represents a profound jurisprudential shift. During earlier times, personal information remained largely siloed within dispersed registries, paper archives and institutional databases characterized by low interoperability. While privacy risks certainly existed, the technical capability to aggregate massive datasets, infer hidden individual attributes and continuously optimize algorithmic decisions across societal sectors was fundamentally constrained. Today, pervasive digital infrastructures capture, aggregate, correlate and process data at a velocity and depth that make the human person unprecedentedly legible to public and private institutions. The rapid advancement of artificial intelligence intensifies this vulnerability by transforming passive data processing into active predictive and classificatory power. Machine learning models do not merely store historical facts, instead they identify complex behavioural patterns, estimate risk probabilities, detect anomalies, automate judgments and allocate societal opportunities. Consequently, individuals are increasingly impacted not just by what they knowingly disclose, but by what algorithmic models infer, predict or statistically associate with them based on collective profiles.

This paradigm shift exposes the structural limits of traditional privacy doctrines, which historically relied on paradigms of secrecy, access control and confidentiality. In an AI-driven society,

an individual may formally consent to share basic data in one context only to suffer downstream harms through behavioural profiling, risk scoring or automated classification in entirely unrelated spheres. Sensitive traits are routinely deduced from seemingly innocuous digital traces without the individual's knowledge or explicit disclosure. Faced with this erosion of individual agency, the legal order must confront a foundational question- Do individuals still possess meaningful self-governance within the digital environment?

This dissertation establishes that the conventional vocabulary of data ownership or consumer choice is inadequate. Instead, the concept of digital self-determination must be elevated to a fundamental constitutional principle. It must be understood not merely as an administrative compliance checkbox, but as a core constitutional mechanism that protects the status of the human person as a sovereign subject of rights rather than a passive object of data driven governance.

The Conceptual Evolution: From Privacy to Digital Self-Determination

To understand the necessity of this constitutional elevation, it is essential to trace how digital self-determination transcends historical privacy paradigms:

- Traditional privacy focused heavily on concealment and the right to be left alone. Digital self-determination, conversely acknowledges that data is continuously in motion and it governs the active cycles of data use, algorithmic inference and systemic governance.

- In complex technological ecosystems, notice and consent models frequently degenerate into an illusion of consent due to severe power imbalances and cognitive opacity. Meaningful self-determination requires structural ex ante safeguards that protect the individual even when formal consent has been technically obtained.

- Constitutional personality and human dignity cannot be reduced to a commercial or proprietary model of data ownership.

- The stakes of AI driven data processing are not merely transactional instead they directly implicate dignity, equality, due process and the structural integrity of democratic self-government.

A constitutional democracy cannot allow the person to become legible, predictable and governable through data without preserving a corresponding sphere of legally protected self-determination.

Comparative Constitutional Doctrinal Analysis

This research utilizes a functional comparative approach, positioning Germany, India and Uzbekistan along a spectrum of constitutional and statutory maturity to evaluate how digital self-determination can operate across diverse legal traditions.

Germany's Informational Self-Determination as a Living Matrix

Germany provides the definitive doctrinal benchmark for this study. The constitutional right to informational self-determination (informationelle Selbstbestimmung) was famously articulated by the Federal Constitutional Court in its 1983 Census Judgment. The Court recognized that unrestricted state data aggregation creates a chilling effect on civic life. Citizens who cannot foresee how their personal data will be utilized will systematically alter their behaviour, self-censor and withdraw from democratic participation. The Court directly anchored this right in the foundational constitutional values of Human Dignity (Article 1(1)) and the Free Development of Personality (Article 2(1)) of the Basic Law for the Federal Republic of Germany (Grundgesetz).

Crucially, German jurisprudence proves that constitutional doctrine can dynamically evolve to confront advanced machine learning systems. The 2023 Constitutional Court decisions concerning

automated police data analysis in Hesse and Hamburg demonstrate rigorous judicial scrutiny over state algorithms. The Court ruled that predictive policing software, by combining and analysing massive state databases to generate risk profiles, constitutes a distinct and severe interference with informational self-determination. This highlights that the doctrine remains a living constitutional shield capable of restraining modern, automated state power.

India's Path from Puttaswamy Case to the DPDP Act, 2023

India represents a fast evolving constitutional landscape characterized by an expansive judicial recognition of privacy that remains partially unfulfilled in its statutory architecture. The Supreme Court's landmark ruling in Justice K. S. Puttaswamy (Retd) v Union of India (2017) firmly established privacy as a fundamental right under Article 21 of the Constitution, explicitly grounding informational control within the concepts of dignity, autonomy and constitutional personhood. Puttaswamy mandated a strict four part proportionality test:

- **Legality:** The state action must be backed by an explicit statutory law.
- **Legitimate Aim:** The restriction must serve a valid, constitutionally permissible objective.
- **Proportionality/Necessity:** The measure adopted must be the least intrusive means available.
- **Procedural Safeguards:** There must be structural mechanisms to prevent institutional abuse.

However, a significant gap persists between this lofty constitutional jurisprudence and its statutory manifestation, the Digital Personal Data Protection (DPDP) Act, 2023. The DPDP Act establishes a foundational compliance regime for digital data, yet it falls short of fully operationalizing digital self-determination in several critical ways:

- The Act permits extensive central government exemptions for state agencies under broad rubrics of sovereignty and public order, bypassing the granular proportionality checks required by the Puttaswamy case.

- Unlike the rigid frameworks of the GDPR or German doctrine, the DPDP Act features a highly flexible purpose limitation standard, leaving significant room for secondary data use and compatible purposes that individuals cannot realistically foresee.

- Unlike Article 22 of the GDPR, the DPDP Act lacks explicit protections against automated profiling, rights to explanation or mandatory human in the loop interventions, creating a vulnerable legal environment as AI tools expand across Indian credit, hiring and public service sectors.

Uzbekistan's Emerging Legislative Framework

Uzbekistan represents an open, developing legal landscape undergoing rapid digital modernization. The baseline framework is anchored by the 2019 Law on Personal Data, which establishes foundational elements of legality, purpose specification and basic data subject rights (which includes access, rectification and erasure). In recent years, Uzbekistan has moved swiftly to formulate AI ethical rules that mandate principles of human centricity, fairness, transparency and explicit human oversight over automated systems. Furthermore, the development of a draft Law on Artificial Intelligence introduces risk based classifications, developer liability and content labelling.

Despite these positive statutory steps, Uzbekistan's framework remains largely under-constitutionalized. The current data protection model operates primarily as a minimalist administrative compliance mechanism rather than a robust expression of fundamental constitutional rights. The integration between ordinary personal data laws and AI ethical rules remains fragmented, lacking

enforceable judicial doctrines that elevate human oversight into a non-negotiable constitutional guarantee.

Conclusion

The age of artificial intelligence represents a critical constitutional moment. As computational architectures expand into the most intimate and public domains of human existence, the legal order cannot remain passive or restrict its focus to narrow statutory compliance.

The comparative analysis of Germany, India and Uzbekistan demonstrates that while institutional histories and legal cultures vary, the underlying threat to human agency remains identical. Whether interpreting Germany's mature census doctrine, realizing the full potential of India's Puttaswamy precedent or guiding Uzbekistan's developing legislative landscape, the fundamental task of modern constitutionalism is clear.

Digital self-determination provides the necessary normative anchor. By recognizing it as a foundational constitutional principle, legal systems can ensure that technological innovation remains structurally accountable to fundamental human rights. Ultimately, this doctrine insists upon a simple, non-negotiable reality- the human person must remain the sovereign, normative centre of digital governance.

Bibliography

1. Access Partnership. (2023). The key policy frameworks governing AI in India. Access Partnership.
2. Bhandari, V., et al. (2017). An analysis of Puttaswamy: The Supreme Court's privacy verdict and its implications. IndraStra Global. SSRN Preprint.
3. Carnegie Endowment. (2024, November 20). India’s advance on AI regulation. Carnegie.
4. Cerberus Legal. (2025, February 12). Uzbekistan moves to regulate Artificial Intelligence (AI) [Client Alert].
5. Corteza Project. (2025, June 9). AI is used to dismantle the human right to privacy. Corteza Project Blog.
6. DRZE – German Reference Centre for Ethics in the Life Sciences. (2023). Informational self-determination [DRZE Research Module].
7. European Court of Human Rights, & Pollicino, O. (2021). Digital private powers exercising public functions – Rule of law challenges [Presentation]. ECHR.
8. European Journal of Law and Technology. (2024). AI governance in India – Law, policy and political economy. European Journal of Law and Technology, 15(2).
9. European Scientific Journal. (2025). AI and cyber-enabled threats to democracy through digital platforms. European Scientific Journal.
10. Government of India. (2025, November 19). Digital Personal Data Protection Act 2023 – Key features. Press Information Bureau.
11. Government of India, Office of Principal Scientific Adviser. (2026, January 22). AI governance through a techno-legal framework [White Paper].
12. Hornung, G., & Schnabel, C. (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. Computer Law & Security Review.
13. Just Access. (2025, January 23). Digital self-determination – Learning to preserve individual dignity and autonomy in an online world. Just-Access Blog.
14. Lakra, R., & Jha, N. (2025). Reclaiming informational self-determination in the DPDPA 2023: A constitutional case for purpose limitation and data minimization. DigiCon Blog / SSRN Working Paper.
15. Lakra, R., & Jha, N. (2026). Re-evaluating publicly available data under the DPDP Act 2023: A constitutional perspective [Draft research paper]. LinkedIn.

16. Law and Tech.ie. (2024, April 21). DPDPA 2023 vs. GDPR: A comparative analysis of India's and EU's data privacy laws. https://lawandtech
17. Limam Blog. (2024, May 21). A quest for the legality of predictive data analytics in law enforcement: Landmark judgment on automated data analysis by the German Federal Constitutional Court. https://limablog
18. Montreal AI Ethics Institute. (2022, February 20). The impact of the GDPR on artificial intelligence. https://montrealethics
19. Nexos AI. (2025, November 16). GDPR for AI: Is your data protected when using AI? [Blog post]. https://nexos
20. Office of the United Nations. (2024, July 24). Risk management profile for AI and human rights. US Dept of State. https://2021-2025.state
21. Operationalizing Digital Self-Determination Collective. (2023). Operationalizing digital self-determination. Data & Policy. Cambridge University Press. https://arxiv
22. Policy Review. (2012). Consent under pressure and the right to informational self-determination. Internet Policy Review, 1(2). https://policyreview
23. Pulatov, K. (2026, January 19). Uzbekistan's Parliament approves Personal Data Law amendments [LinkedIn post]. LinkedIn. https://linkedin
24. Rakhmatov, R. (2025, April 26). AI policy in Uzbekistan: Should we follow global models or our own path? [LinkedIn article]. LinkedIn. https://linkedin
25. Retskraft, & Şerbanescu, B. (2024). Why does artificial intelligence challenge democracy? Retskraft Journal, 5(1). https://retskraft
26. RSIS International. (2024). The impact of artificial intelligence on privacy laws. International Journal of Research and Innovation in Social Science (IJRISS). https://rsisinternational
27. Sage Journals. (2025). India's AI regulation at the crossroads: A comprehensive assessment. Indian Journal of Law and Technology. https://journals.sagepub
28. Sanjar. (2025). Regulating artificial intelligence in Uzbekistan. ICAS Conference Proceedings. Inlibrary.uz. https://inlibrary
29. State Department of the United States. (2024, July 24). Risk management profile for AI and human rights. https://2021-2025.state
30. Swiss Data Alliance. (2013). Definition: Digital self-determination (Glossary entry). https://swissdataalliance
31. TandF Cogent Social Sciences. (2025). Reflections on the data protection compliance of AI systems. Cogent Social Sciences. https://tandfonline
32. United Nations / EJIL:Talk!. (2025, November 11). A human right to informational self-determination: What it is and why it matters for digital human rights. https://ejiltalk
33. Uzbekistan. (2026). Law 'On Personal Data' (as amended by Law No. 1125 and subsequent amendments, including 2026 clarification of storage and localisation rules). https://blackswan
34. Uzbekistan AI Ethical Rules. (c. 2023–2024). Ethical rules for the use of artificial intelligence (Government resolution). https://cerberus
35. Vakhidov Law. (2025). Legislative updates in the field of artificial intelligence and personal data regulation in Uzbekistan (Firm Newsletter). https://vakhidovlaw
36. VivaTech. (2026, March 18). The impact of AI on democracy: Risks and opportunities. https://vivatech
37. World State of AI Initiative / IITM. (2025). Making AI self-regulation work (Policy paper). https://wsai.iitm.ac
38. Yale Journal of Law and Technology. (c. 2024–2025). Artificial intelligence: Risks to privacy and democracy. Yale Journal of Law and Technology (YJoLT). https://yjolt